

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

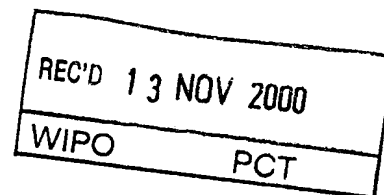
IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

**THIS PAGE BLANK (USPTO)**

**PRV**PATENT- OCH REGISTRERINGSVERKET  
Patentavdelningen

SE00/1847



4

**Intyg  
Certificate**

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

*This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.*

(71) Sökande SAAB AB, Linköping SE  
Applicant (s)

(21) Patentansökningsnummer 9903422-5  
Patent application number

(86) Ingivningsdatum 1999-09-22  
Date of filing

Stockholm, 2000-10-31

För Patent- och registreringsverket  
For the Patent- and Registration Office

*A. Södervall*  
Anita Södervall

Avgift  
Fee

## PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

si/lt

ref. SE 51034

5 Sökande: SAAB AB

### Datoranordning med säkerhetsfunktion

#### 10 UPPFINNINGENS BAKGRUND OCH TIDIGARE TEKNIK

Föreliggande uppfinning avser en datoranordning med säkerhetsfunktion för att undvika ej nödvändig nedkoppling av datoranordningen, innefattande processororgan, en ordinarie minnesenhet ansluten till nämnda processororgan och inrättad att innehålla åtminstone ett program som exekveras av processororganet, en övervakningsenhet som övervakar datoranordningens funktion och som är inrättad att, om fel uppstår, sända en återstartsignal eller stoppsignal till processororganet.

20 Sådana datoranordningar är tidigare kända. Övervakningsenheten kan exempelvis utgöras av en så kallad "watchdog timer". US-A-4 763 296 beskriver funktionen av en sådan watchdog timer. En sådan anordning har således en timer som kontinuerligt är i drift när datoranordningen används. Om timern uppnår ett förutbestämt värde, dvs om en förutbestämd tid har löpt ut, så genererar watchdog-timern en återstartsignal som förorsakar en återstart (reset) av datoranordningen. Under normal användning nollställs timern med jämna mellanrum av processorns normala programförlopp. Om fel skulle uppstå, exempelvis om datorn exekverar en oändlig subrutin, nollställs inte timern och watchdog-timern förorsakar således en omstart av systemet.

35 Även andra typer av datoranordningar med säkerhetsfunktioner är förut kända. Således beskriver EP-A-481 508 en anordning som innefattar ett backup-minne. När strömförsörjningen stängs

- av till datoranordningen öv rförs centralprocessorns status och innehållet i ett huvudminne till nämnda backup-minne. När sedan datoranordningen åter startas genom att strömförsörjningen ansluts på nytt så återställs vad som finns lagrat i backup-minnet.
- 5

- EP-A-265 366 beskriver en datoranordning som innefattar ett primärt minne och ett backup-minne. Omkoppling från det primära minnet till backup-minnet görs med hjälp av en "Backup Control System Transfer Mechanism". Denna mekanism är relativt komplicerad. Vid generering av en power-on-reset signal säkerställer nämnda mekanism att omstart sker från primärminnet (se spalt 6, rad 21-28).
- 10
- 15 Det föreligger ett behov av att förbättra säkerhetsfunktionen hos en datoranordning. Sålunda finns ett behov att på ett säkert sätt omstarta datoranordningen när ett fel har detekterats. Ett sådant fel som kan förorsaka fel i datorns drift är exempelvis minnesfel som kan uppträda i det minne där program finns lagrade som
- 20
- exekveras i datoranordningen. Fel kan även förorsakas av programvaran som finns lagrad i datoranordningens minne. Exempelvis kan sådana fel uppstå om ny programvara används som inte är fullständigt utprovad. Vidare finns ett behov av att säkerställa funktionen hos datoranordningen med relativt enkla medel. Ett ytterligare problem är att säkerställa åtminstone vissa
- 25
- basfunktioner hos datoranordningen när olika fel uppstår.

#### SAMMANFATTNING AV UPPFINNINGEN

- 30 Ändamålet med föreliggande uppfinning är att åstadkomma en datoranordning med en tillförlitlig säkerhetsfunktion som dessutom uppnås med relativt enkla medel.

- 35 Detta ändamål uppnås med den inledningsvis angivna datoranordningen som kännetecknas av en ytterligare minnesenhet som är inrättad att innehålla åtminstone vissa grundläggande sy-

steminstruktioner, varvid datoranordningen är inrättad så att processororganet, vid återstart genererad av nämnda återstartsignal från övervakningsenheten, kopplas upp mot den ytterligare minnesenheten och läser och exekverar instruktioner som  
5 finns lagrade i denna, medan den ordinarie minnesenheten är bortkopplad från processororganet.

---

Genom att processororganet kopplas upp mot den ytterligare minnesenheten när en återstartsignal har genererats av övervakningsenheten så undviks att eventuella fel som föreligger i  
10 de instruktioner som är lagrade i den ordinarie minnesenheten överförs till processororganet. Därigenom uppnås en säkrare omstart av datoranordningen efter det att en återstartsignal har genererats som svar på ett detekterat fel. I detta sammanhang  
15 bör noteras att när i patentkraven och beskrivningen anges att en minnesenhet kopplas upp eller är bortkopplad från processororganet så menas därmed inte nödvändigtvis att bortkoppling sker genom att fysiskt bryta förbindelsen mellan processororganet och minnesenheten i fråga. Begreppen koppla upp och bortkoppla  
20 innefattar således två möjligheter: dels fysisk koppling genom brytning av förbindelsen, dels uppkoppling och bortkoppling på programnivå.

Enligt en utföringsform av uppfinningen utgör den ordinarie minnesenheten och den ytterligare minnesenheten två olika, fysiskt separata, minnen. Därigenom uppnås ökad säkerhet eftersom den ordinarie minnesenheten föreligger som ett separat minne som är helt bortkopplat från processororganet vid återstart.  
25

Enligt en alternativ utföringsform av uppfinningen utgör den ordinarie minnesenheten och den ytterligare minnesenheten två delar av fysiskt samma minne, men med olika minnesadresser. Genom denna konstruktion krävs färre minneskomponenter eftersom den ytterligare minnesenheten finns lagrad som en speciell del av det minne där även den ordinarie minnesenheten ingår.  
30  
35

Enligt en ytterligare utföringsform av uppfinningen är nämnda övervakningsenhet inrättad att generera en signal i beroende av en timer på så sätt att nämnda återstartsignal genereras om  
5 ingen trigger-signal som nollställer timern erhålls inom ett förutbestämt tidsintervall. Övervakningsenheten kan i detta fall således utgöras av en så kallad watchdog timer (WDT). En sådan WDT ingår ofta i datoranordningar. Således kan en sådan väl fungerande redan befintlig WDT användas som övervakningsenhet  
10 i anordningen enligt föreliggande uppfinning. Det bör dock påpekas att även andra typer av övervakningsenheter än en WDT kan användas i datoranordningen enligt uppfinningen.

Enligt ännu en utföringsform av uppfinningen innefattar datoranordningen en minnessäkerhetskrets som är inrättad att stoppa  
15 inläsning från den ordinarie minnesenheten och att koppla upp för inläsning från nämnda ytterligare minnesenhet när både nämnda återstartsignal och en signal indikerande pålagd drivspänning föreligger. En sådan minnessäkerhetskrets är en relativt enkel och väl fungerande krets som tillser att omkoppling  
20 från den ordinarie till den ytterligare minnesenheten sker. Vidare säkerställer denna minnessäkerhetskrets att en sådan omkoppling endast sker om drivspänning till datoranordningen föreligger.

25 Enligt en ytterligare utföringsform av uppfinningen är nämnda ytterligare minnesenhet inrättad så att den innehåller grundläggande systeminstruktioner men en hög nivå av funktionssäkerhet. Den ytterligare minnesenheten kan härvid vara inrättad  
30 att innehålla systeminstruktioner som redan har varit väl testade och som därför har en hög funktionssäkerhet. Den ytterligare minnesenheten kan härvid också vara försedd med de grundläggande instruktionerna för datoranordningen medan icke nödvändiga systeminstruktioner har uteslutits från nämnda ytterli-  
35 gare minnesenhet.

Enligt ännu en utföringsform av uppfinningen är nämnda ytterligare minnesenhet inrättad så att den inn håller syst minstruktio-  
tioner med en nivå av funktionssäkerhet som är högre än den  
5 nivå av funktionssäkerhet som föreligger i den ordinarie minnes-  
enheten. Således kan den ordinarie minnesenheten innefatta sy-  
steminstruktioner som ej är så väl testade i datoranordningen.

Den ytterligare minnesenheten kan därvid innehålla de grund-  
läggande systeminstruktionerna som redan har visat sig ha hög  
funktionssäkerhet. Inom uppfinningens ram ligger givetvis även  
10 möjligheten att den ordinarie minnesenheten och den ytterligare  
minnesenheten innehåller systeminstruktioner med samma nivå  
av funktionssäkerhet.

Enligt en ytterligare utföringsform av uppfinningen är åtminstone  
15 nämnda ytterligare minnesenhet ett icke flyktigt minne. Detta bi-  
drar till en ökad funktionssäkerhet hos datoranordningen.

Enligt ännu en utföringsform av uppfinningen innefattar nämnda  
processororgan ett arbetsminne som är så inrättat att vid åter-  
20 start av datoranordningen nollställs detta arbetsminne innan in-  
läsning från nämnda ytterligare minnesenhet påbörjas. Därige-  
nom säkerställs att instruktioner som kan innehålla fel och som  
härör från den ordinarie minnesenheten ej kvarligger i arbets-  
minnet innan inläsning från den ytterligare minnesenheten på-  
25 börjas.

Enligt en ytterligare utföringsform av uppfinningen är nämnda  
ytterligare minnesenhet inrättad att vara skrivskyddad åt-  
30 minstone då datoranordningen är i drift. Detta bidrar till ytterli-  
gare säkerhet eftersom innehållet i den ytterligare minnesenhe-  
ten är skyddat och ej kan ändras då datoranordningen är i drift.

Enligt ännu en utföringsform av uppfinningen är datoranord-  
ningen inrättad så att om nämnda återstartsignal har genererats  
35 ett förutbestämt antal gånger, så genereras, om åter ett fel upp-  
står, nämnda stoppsignal. Detta innebär att övervakningsenhe-



ten genererar ett förutbestämt antal återstartssignaler. Om det visar sig att fel föreligger även efter det att ett förutbestämt antal återstartförsök har gjorts så stoppas datoranordningen.

- 5 Enligt ännu en utföringsform av uppfinningen innefattar datoranordningen omkopplingsorgan för att manuellt generera nämnda återstartssignal. Detta innebär att förutom automatisk generering av återstartssignal genom övervakningsenheten kan även en manuell återstartssignal genereras av en operatör. En operatör kan  
10 således beordra att återstart från den ytterligare minnesenheten ska ske.

#### KORT BESKRIVNING AV RITNINGEN

- 15 Föreliggande uppfinning skall nu förklaras med hjälp av en beskriven utföringsform, som utgör ett exempel på uppfinningen, och med hänvisning till den bifogade ritningen.

- 20 Fig 1 visar schematiskt ett blockschema av en utföringsform av uppfinningen.

#### DETALJERAD BESKRIVNING AV EN UTFÖRINGSFORM AV UPPFINNINGEN

- 25 Fig 1 visar ett blockschema av en utföringsform av uppfinningen. Datoranordningen innefattar ett processororgan 10. Med detta processororgan 10 avses inte endast datoranordningens centrala processorenhet (CPU) utan även andra centrala delar av datoranordningen såsom exempelvis arbetsminnet 22. Datoranordningen innefattar även en ordinarie minnesenhet 12. Denna ordinarie minnesenhet 12 kan exempelvis utgöras av någon form av PROM, exempelvis UVPROM, EEPROM eller liknande. När datoranordningen först startas uppkopplas processororganet 10  
30 mot den ordinarie minnesenheten 12. Denna ordinarie minnesenhet 12 är således inrättad att innehålla de instruktioner  
35 som styr datoranordningens drift. Datoranordningen innefattar

även en övervakningsenhet 14. Övervakningsenheten 14 övervakar datoranordningens funktion och är inrättad att generera en återstartsignal eller stoppsignal till processororganet 10 om övervakningsenheten 14 detekterar ett fel. Övervakningsenheten 5 14 kan exempelvis utgöras av en så kallad watchdog timer (WDT). En sådan WDT 14 genererar en signal som beror av en timer 18. En återstartsignal genereras därvid om WDT:n 14 inom ett förutbestämt tidsintervall inte erhåller en trigger-signal som nollställer timern 18. För att ha hög säkerhet innefattar WDT:n 10 14 lämpligen en egen timer 18. Det är dock möjligt att WDT:ns 14 timer-funktion styrs av samma klocka som ingår i processororganet 10.

Datoranordningen innefattar även en ytterligare minnesenhet 16. 15 Denna ytterligare minnesenhet 16 är inrättad att innehålla åtminstone vissa grundläggande systeminstruktioner. Den ytterligare minnesenheten 16 kan utgöra ett minne som är fysiskt separat från den ordinarie minnesenheten 12. Det är även möjligt att den ordinarie minnesenheten 12 och den ytterligare minnes- 20 enheten 16 utgör två delar av fysiskt samma minne. För att ytterligare öka säkerheten om ett minnesfel skulle uppstå kan den ordinarie minnesenheten 12 och den ytterligare minnesenheten 16 utgöras av fysiskt separata minnen av olika typ, exempelvis från olika tillverkare. Den ytterligare minnesenheten utgörs 25 lämpligen av någon form av PROM, exempelvis UVROM eller EEPROM.

Datoranordningen innefattar även en minnessäkerhetskrets 20. 30 Denna minnessäkerhetskrets 20 kan ingå som en del av processororganet 10. I den visade utföringsformen utgör emellertid minnessäkerhetskretsen 20 en separat krets. Minnessäkerhetskretsen 20 innefattar en AND-grind 21. Minnessäkerhetskretsen 20 styr vilken av den ordinarie minnesenheten 12 och den ytterligare minnesenheten 16 som skall vara inkopplad till processor- 35 organet 10. Denna styrning kan antingen utgöras av brytning eller slutning av den elektriska förbindelsen mellan respektive

minn senhet 12, 16 och processorenheten 10 eller också utgö-  
ras av styrning på programnivå av dessa förbindelser. Det är  
även möjligt att styrningen utgörs av en kombination av pro-  
gramvaruinstruktioner och fysisk brytning eller slutning. AND-  
5 grindens ena ingång är ansluten till en ledning 23 som indikerar  
att drivspänning föreligger. AND-grindens 21 andra ingång är  
ansluten till en ledning 25 som är förbunden med WDT:n 14. Via  
denna ledning 25 leds en av WDT:n 14 genererad återstartsignal  
till AND-grinden 21 och därmed till minnessäkerhetskretsen 20.

10

Datoranordningen innefattar även ett omkopplingsorgan 24 för  
att manuellt generera en återstartsignal. Detta omkopplingsor-  
gan 24 kan lämpligen vara anslutet till den ingång hos AND-  
grinden som även är ansluten till WDT:n 14.

15

WDT:n 14 övervakar således datoranordningens funktion. När  
datoranordningen fungerar normalt erhåller WDT:n 14 med  
jämna mellanrum en trigger-signal från processororganet 10.  
Denna trigger-signal nollställer timern 18. Därvid genererar  
20 WDT:n 14 ingen återstartsignal till ledningen 25. Om emellertid  
fel uppstår så att WDT:n 14 ej erhåller någon trigger-signal inom  
ett förutbestämt tidsintervall från processororganet 10 så gene-  
rerar WDT:n 14 en återstartsignal. Denna återstartsignal leds  
således till den ena ingången hos AND-grinden 21. När AND-  
25 grinden 21 erhåller en sådan återstartsignal, och om samtidigt  
AND-grindens 21 andra ingång detekterar att drivspänning före-  
ligger, så tillser minnessäkerhetskretsen 20 att den ordinarie  
minnesenheten 12 kopplas bort från processororganet 10 och att  
den ytterligare minnesenheten 16 kopplas upp mot processoror-  
ganet 10. Även processororganet 10 erhåller en signal, lämpli-  
30 gen från WDT:n 14, om att återstart skall genomföras. Proces-  
sororganets 10 arbetsminne 22 nollställs därvid, varefter inläs-  
ning från den ytterligare minnesenheten 16 sker. Inläsning sker  
därvid till förutbestämda adresser hos arbetsminnet 22. Proces-  
35 sororganet 10 läser och exekverar således de instruktioner som  
finns lagrade i den ytterligare minnesenheten 16.

Det är tänkbart att ett återstartförsök misslyckas och att WDT:n 14 därför genererar en ny återstartsignal. Om ånyo fel detekteras kan ytterligare återstartsignaler genereras av WDT:n 14.

5 Datoranordningen är därvid lämpligen inrättad så att när ett förutbestämt antal återstartförsök har gjorts så stoppas återstartförsöken. Därvid kan en varningsfunktion genereras av datoranordningen och senaste information beträffande processororgans 10 och minnesenheter 12, 16 status kan registreras för senare analys. Lämpligen är datoranordningen inrättad så att återstartförsöken stoppas efter exempelvis ett till fyra återstartförsök, företrädesvis efter två återstartförsök. Datoranordningen kan därvid vara inrättad så att återstartförsöken stoppas om nämnda förutbestämda antal återstartförsök har genomförts

15 inom ett förutbestämt tidsintervall.

För ökad säkerhet är lämpligen den ytterligare minnesenheten 16 inrättad så att den är skrivskyddad när datoranordningen är i drift. Vidare utgörs lämpligen såväl den ordinarie minnesenheten 20 12 som den ytterligare minnesenheten 16 av icke flyktiga minnen.

Den ytterligare minnesenheten 16 är lämpligen inrättad så att den innehåller grundläggande systeminstruktioner vid en hög nivå av funktionssäkerhet. Den ytterligare minnesenheten 16 kan därvid innehålla primära och välutprovade systemfunktioner. Lämpligen är den ytterligare minnesenheten 16 inrättad så att den därvid innehåller systeminstruktioner med en högre nivå av funktionssäkerhet än de systeminstruktioner som föreligger i den ordinarie minnesenheten 12. Med uttrycket "nivå av funktionssäkerhet" kan härvid exempelvis avses de programvarusäkerhetsnivåer som definierats enligt RTCA-standard dokument NO.RTCA/DO-178B.

25

30

Föreliggande uppfinning är inte begränsad till den visade utföringsformen utan kan varieras och modifieras inom ramen för de efterföljande patentkraven.

---

# Patentkrav

1. Datoranordning med säkerhetsfunktion för att undvika ej  
nödvändig nedkoppling av datoranordningen, innefattande  
5 processororgan (10),  
en ordinarie minnesenhet (12) ansluten till nämnda pro-  
cessororgan (10) och inrättad att innehålla åtminstone ett pro-  
gram som exekveras av processororganet (10),  
en övervakningsenhet (14) som övervakar datoranordning-  
10 ens funktion och som är inrättad att, om fel uppstår, sända en  
återstartsignal eller stoppsignal till processororganet (10),  
kännetecknad av  
en ytterligare minnesenhet (16) som är inrättad att inne-  
hålla åtminstone vissa grundläggande systeminstruktioner, var-  
15 vid datoranordningen är inrättad så att processororganet (10),  
vid återstart genererad av nämnda återstartsignal från övervak-  
ningsenheten (14), kopplas upp mot den ytterligare minnesen-  
heten (16) och läser och exekverar instruktioner som finns lag-  
rade i denna, medan den ordinarie minnesenheten (12) är bort-  
20 kopplad från processororganet (10).
2. Datoranordning enligt krav 1, varvid den ordinarie minnes-  
enheten (12) och den ytterligare minnesenheten (16) utgör två  
25 olika, fysiskt separata, minnen.
3. Datoranordning enligt krav 1, varvid den ordinarie minnes-  
enheten (12) och den ytterligare minnesenheten (16) utgör två  
delar av fysiskt samma minne, men med olika minnesadresser.
- 30 4. Datoranordning enligt något av föregående krav, varvid  
nämnda övervakningsenhet (14) är inrättad att generera en sig-  
nal i beroende av en timer (18) på så sätt att nämnda återstart-  
signal genereras om ingen trigger-signal signal som nollställer  
timern (18) erhålls inom ett förutbestämt tidsintervall.

35

5. Datoranordning enligt något av föregående krav, innefattande en minnessäkerhetskrets (20) som är inrättad att stoppa inläsning från den ordinarie minnesenheten (12) och att koppla upp för inläsning från nämnda ytterligare minnesenhet (16) när
- 5 både nämnda återstartsignal och en signal indikerande pålagd drivspänning föreligger.
- 
6. Datoranordning enligt något av föregående krav, varvid nämnda ytterligare minnesenhet (16) är inrättad så att den
- 10 håller grundläggande systeminstruktioner med en hög nivå av funktionssäkerhet.
7. Datoranordning enligt krav 6, varvid nämnda ytterligare minnesenhet (16) är inrättad så att den innehåller systeminstruktioner men en nivå av funktionssäkerhet som är högre än
- 15 den nivå av funktionssäkerhet som föreligger i den ordinarie minnesenheten (12).
8. Datoranordning enligt något av föregående krav, varvid åtminstone nämnda ytterligare minnesenhet (16) är ett icke flyktigt minne.
- 20
9. Datoranordning enligt något av föregående krav, varvid nämnda processororgan (10) innefattar ett arbetsminne (22)
- 25 som är så inrättat att vid återstart av datoranordningen nollställs detta arbetsminne (22) innan inläsning från nämnda ytterligare minnesenhet (16) påbörjas.
10. Datoranordning enligt något av föregående krav, varvid nämnda ytterligare minnesenhet (16) är inrättad att vara skrivskyddad åtminstone då datoranordningen är i drift.
- 30
11. Datoranordning enligt något av föregående patentkrav, inrättad så att om nämnda återstartsignal har genererats ett förutbestämt antal gånger så genereras, om åter ett fel uppstår, nämnda stoppsignal.
- 35

12. Datoranordning enligt något av föregående krav, innefattande omkopplingsorgan (24) för att manuellt generera nämnda återstartsignal.



**Sammandrag**

- Uppfinningen avser en datoranordning med säkerhetsfunktion för att undvika ej nödvändig nedkoppling av datoranordningen.
- 5 Datoranordningen innefattar processororgan (10), en ordinarie minnesenhet (12), en övervakningsenhet (14) och en ytterligare minnesenhet (16). Datoranordningen är inrättad så att proces-
- 
- 10 sororganet (10) vid en återstart genererar av en återstartsignal, kopplas upp mot den ytterligare minnesenheten (16) och läser och exekverar de instruktioner som finns lagrade i denna, medan den ordinarie minnesenheten (12) är bortkopplad från processororganet (10).

(Fig 1)

1/1

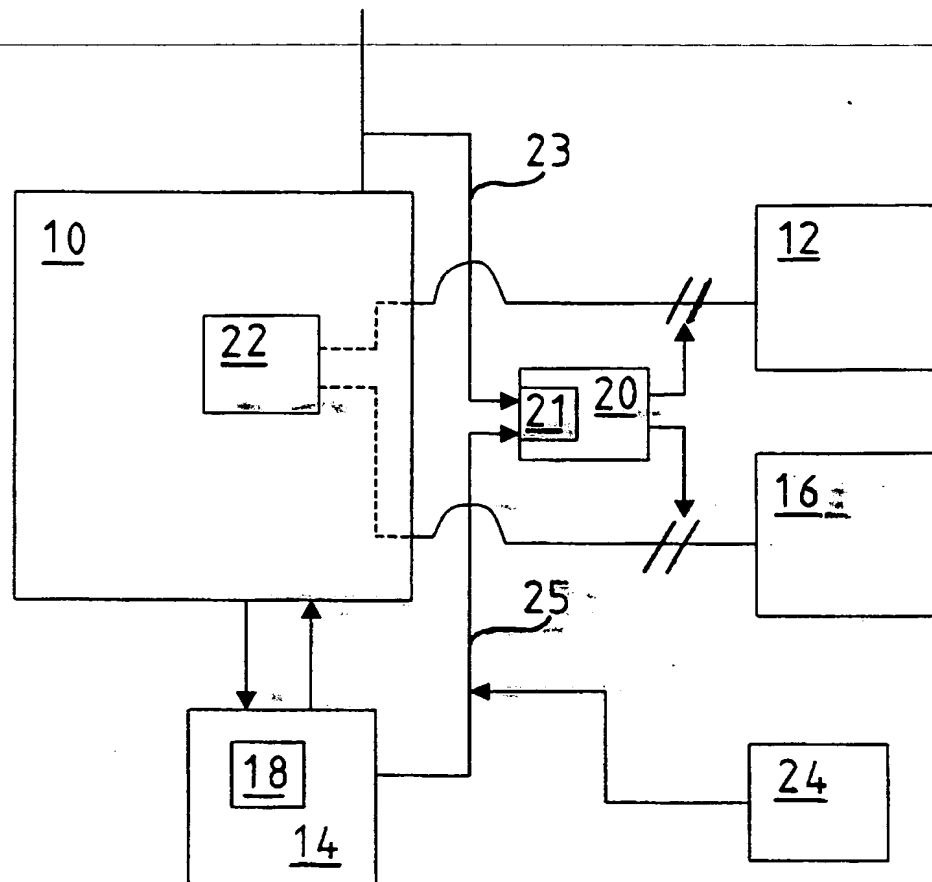


FIG 1